This listing of claims will replace all prior versions and listings of claims in this application:

Listing of Claims

1. (Currently amended) A method for transmitting data in an IP network ~~according to a source and destination flow table, a flow key, and one or more variables~~ comprising:

receiving a data transmission in ~~an~~ the IP network;

extracting ~~at least one field~~ a source address, a destination address, and at least one port from a header of the data transmission;

~~forming a combined, source/destination address entry based on the extracted at least one field;~~

looking up the source address and the destination address in an address mask table and determining a most granular bit-value mask by finding a longest prefix match corresponding to ~~the combined, source/destination address entry from a~~ each of the source address and the destination address to obtain address result values, the address mask table having a plurality of bit-value masks ~~by performing a logical AND operation on bits in the network~~, wherein the plurality of bit-value masks ~~include~~ have a plurality of granularities ~~corresponding to each of the plurality of fields in the header~~;

looking up the at least one port in a port mask table to obtain port result values;

~~applying the determined bit-value mask to the combined, source/destination address entry;~~

forming a source and destination and port flow key based on ~~the application of the determined bit-value mask to combined, source/destination address entry~~ the address result values and the port result values;

~~indexing the source and destination flow table with reference to the masked flow key;~~

looking up a flow ~~entry~~ key in ~~the indexed~~ a source and destination and port flow table to find a corresponding flow entry; and

if the flow entry indicates to deny the data transmission, blocking the data transmission, otherwise transmitting the data transmission in the IP network with a service profile specified by ~~according to~~ the flow entry.

2. (Cancelled)

3. (Currently amended) The method according to claim 1, further comprising:

if no bit-value mask in ~~a~~ the address mask table corresponds to the source address or the destination address ~~at least one extracted field~~, no mask is applied to the source address or the destination address ~~at least one field~~.

4. (Currently amended) The method according to claim 3, further comprising:

if no flow entry corresponds to the formed flow key, a default value is used for the flow entry.

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Previously presented) The method according to claim 1, further comprising:

entering a bit-value mask in the mask table by a service provider.

9. (Currently amended) The method according to claim 1, wherein the bit-value mask in the mask table corresponds to a range of a plurality of subscribers to a service.

10. (Previously presented) The method according to claim 9, wherein the plurality of subscribers includes at least one selected from a group consisting of network hosts and a sub-network.

11. (Previously presented) The method according to claim 1, wherein the bit-value mask corresponds to at least one network application.

12. (Previously presented) The method according to claim 1, wherein the flow entry includes transmission information.

13. (Currently amended) The method according to claim 12, wherein the transmission information includes at least one selected from a group consisting of application specific qualities ~~an~~ and service specific qualities.

14. (Previously presented) The method according to claim 13, wherein the transmission information includes at least one selected from a group consisting of policy, quality of service, and latency.

15. (Currently amended) A system for transmitting data ~~according to a flow table, a flow key, and one or more variables, the system~~ comprising:

a receiving unit configured to receive a data transmission in an IP network;

an extraction unit configured to extract ~~at least one field~~ a source address, a destination address, and at least one port from a header of the data transmission;

~~an address entry unit configured to form a combined, source/destination address from the extracted at least one field;~~

a mask table including a plurality of bit-value masks, wherein the plurality of bit-value masks include a plurality of granularities ~~corresponding to each of the plurality of fields in the header~~;

a masking unit configured to determine a most granular bit-value mask by finding a longest prefix match corresponding to each of the source address and the destination address ~~the combined, source/destination address from the mask table by performing a logical AND operation on bits in the network, apply the determined bit-value mask to the combined, source/destination address,~~ and finding a match for the port and output a masked flow key based on the matches;

a flow table indexed with reference to the masked flow key; and

a transmitter configured to transmit the data transmission in an IP network according to a flow entry in the flow table corresponding to the masked flow key of the data transmission.

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Previously presented) The method according to claim 15, wherein the bit value mask is configured to allow at least one bit-value mask to be entered by a service provider.